Investigations of a Multi-Cell Wireless LAN Under Different Load Distributions

By:
Nazim Farouk Idris Habbani

A Thesis submitted in partial fulfillment of the Requirements of the Master degree in Computer Architecture and Networks

Supervised By:
Dr. Mohammed Ali Hamad Abbass

Department of Electrical & Electronic Engineering
Faculty of Engineering & Architecture
University of Khartoum
November 2004

CONTENTS

DEDICATION

God has blessed me with a wonderful family and nice friends to whom this thesis is dedicated.

To my father, my mother, my brothers and sisters and my friends.

ACKNOWLEDGEMENTS

I would like to express my deep thanks and gratitude to my thesis research supervisor Dr. Mohammed Ali H. Abbass who kindly guided me throughout my research, and advised me a lot. I also thank Ustaz Mohammed A/ Moniem Karrouri, Computer Laboratory Supervisor for Post-Graduate Studies, Electrical & Electronics Department. Also I am grateful to Eng. Khalid Hussien Elfaki for his help. Finally, I would like to thank the staff of the Electrical & Electronics Department for their valuable help throughout my study for both B.Sc. and M.Sc. degrees.

ABSTRACT

Wireless local area networks are gaining popularity at unprecedented rates at homes and at offices. They do have advantages over those of different types of wired networks, especially for small application area of LANs.

This thesis investigates multi cell wireless LANs under different load distributions. A model was assumed, and on the basis of this model a C++ simulation software was implemented to study the behavior of a small ad hoc wireless LAN consisting of five hosts that share the transmission media. They are distributed at different basic service sets (BSS) and each one represents an access point (AP), transmitting packets to others. The message duration and inter-arrival time units were assumed to follow exponential distribution (Probability density function). Residual errors

were introduced in the channels that are due to noise, interference and other propagation effects in the software as random possibilities. The throughput and average delay per packet of the transmission medium are printed for different parameters, including the constant of the reciprocal of the probability density function (λ) of the inter-arrival time of the messages which represents the load in the wireless network simulation.

The results for the throughput and the delay were found closed to the expected values using this simulation software. But the results show some limitation in the wireless control access MAC CSMA/CA protocol for the wireless LANs which is defined by the international organizations. It is recommended for further work on this field of studies to add some new statements in the CSMA/CA protocol to achieve higher utilization for the wireless LANs for small area applications, such as in homes, offices and small university campuses.

ABSTRACT(ARABIC)

مستخلص :

تكتسب الشّبكات المحلية آللا سلكيه شعبية بمعدلات غير مسبوقة في البيوت وفى المكاتب. إذ أن لد يها ميزات على الأنواع المختلفة للشبكات السلكية بخاصة في التطبيقات الصغيرةا للشبكات المحلية

تبحث هذه الرسّالة في شبكات محلية لاسلكية ذات خلا يا متعددة تحت توزيعات حمل مختلفة. لقد تم افتراض نموذج ، وعلى أساس هذا النموذج تم وضع برامج محاكاة باستخدام لغة C++ لدراسة السّلوك لشبكة محليّة لا سلكية افتراضية تتكونّ من خمسة مضيفين يتقاسمون قناة الإرسال . وهم موزعون في أجهزة الخدمة الأساسية المختلفة (BSS) ، وكلّ واحد يمثّل نقطة مدخل (AP) تنتقل منه الحزم إلى الآخرين . مّدة الرّسالة ووحدات وقت الوصول افترضت أن تتبع التّوزيع المطّرد (دالة كثافة الاحتمالات) . كم افترضت الأخطاء في في قنوات الارسال بسبب الضوضاء أو التّداخّل أو اثار النّشر الأخرى في البرامج كاحتمالات عشوائيّة . الكفاءة والتأخير لكل حزمة لقناة الإرسال يتم الحصول عليها للمعامل المختلفة ، ومن ثم طباعتها ، متضمنة معكوس ثابت دالة كثافة الاحتمالات (λ) لوقت الوصول للرسائل التي تمثّل الحمل في تمثيل الشبكة اللاسلكية.

النتائج للكفاءة و التأخير لكل حزمة وجدت لتكون قريبة من القيم المتوقعة لبرنامج المحاكاة هذا. أظهرت النتائج أن هنالك حوجة لاضافة بعض الخيارات في برتوكول التحكم في مدخل السّيطرة اللاسلكي للشّبكات المحلية(CSMA/CA MAC Protocol) التي تعرّف بواسطة منظمات الاتصالات الدوليّة.

يقترح للعمل الإضافي في هذا المجال إضافة بعض الفقرات الجديدة في برتوكول (CSMA/CA MAC Protocol) لتحقيق استغلال امثل للشبكات المحليّة اللاسلكية للتطبيقات في المناطق الصغيرة، مثل البيوت و المكاتب و المجمعات الجامعية الصغيرة.

CHAPTER ONE

INTRODUCTION

1.1 OVERVIEW:

A wireless LAN (Local Area Network) is one that makes use of a wireless transmission medium. In the past wireless LANs were little used. This was due to various reasons, including high prices, low data rates, occupational safety concerns, and licensing requirements. Later on the problems have been addressed and the popularity of wireless LANs has grown rapidly.

1.2 WIRELESS LAN APPLICATIONS:-

There are four application areas for wireless LANs: LAN extension, cross building inter-connects, nomadic access, and ad hoc networks.

1.2.1 LAN Extension:

The wireless products that appeared in the late 1980s were used as substitutes for traditional wired LANs. A wireless LAN needs less cost for the installation of cabling and it is easy in relocation and other modifications to network structure. The requirement for wireless LANs was delayed due to some reasons. Firstly, architects usually include in their design of new buildings pre-wiring for data applications. Secondly, as there was a development in data transmission technology, there was an increasing reliance on twisted pair cabling for LANs and, in particular, Category 3 and Category 5 unshielded twisted pair. Thus, the use of a wireless LAN to replace the wired LAN has not happened as quickly as was expected..

However, in especial cases, there was a need for the wireless LAN as an alternative to a wired LAN. Examples include buildings with large open areas, such as manufacturing plants, stock exchange trading floors, and warehouses; historical buildings with insufficient twisted pair and where drilling holes for new wiring is prohibited; and small offices where installation and maintenance of wired LANs is not economical. In such cases, an organization will also have a wired LAN to support servers and some stationary workstations. For example, a manufacturing plant, which has an office area that is

separate from the factory floor but that, must be linked to it for networking purposes. In such a case a wireless LAN will be linked together with a wired LAN. Such an application area is known as LAN extension.

Figure 1.1 indicates a simple wireless LAN configuration that is typical of many environments. There is a backbone wired LAN, such as Ethernet, that supports servers, workstations, and one or more bridges or routers to link with other networks. In addition, there is a control module (CM) that acts as an interface to a wireless LAN. The control module includes either a bridge or router functionality to link the wireless LAN to the backbone. It includes some sort of access from the end systems. Note that some of the end systems are stand-alone devices such as a workstation or a

server. Hubs or other user modules (UMs) that control a number of stations off a wired LAN may also be part of the wireless LAN configuration.

The configuration of Figure 1.1 can be referred to as a single-cell wireless LAN; all of the wireless end systems are within range of a single control module. Another common configuration, suggested by **Figure 1.2**, is a multiple-cell wireless LAN. In this case, there is multiple control modules interconnected by a wired LAN. Each control module supports a number of wireless end systems within its transmission range. For example, with an infrared LAN, transmission is limited to a single room; therefore, one cell is needed for each room in an office building that requires wireless support [1].

1.2.2 Cross-Building Interconnects:

One use of wireless LAN technology is to connect LANs in neighboring buildings, whether they are wired or wireless. In the latter case, a point-to-point wireless link is used between two buildings. The devices that are used are bridges or routers. This single point-to-point link is not a LAN, but it is usual to include this application under the heading of wireless LAN.

1.2.3 Nomadic Access:

Nomadic access provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna, such as a laptop computer. One example for such a connection is to enable an employee to transfer data from a personal portable computer to a server in the office. Nomadic access is also useful in an extended environment such as a campus or a business operating out of a cluster of buildings. In both of these cases, users may move around with their portable computers and may wish access to the servers on a wired LAN from various locations.

1.2.4 Ad Hoc Networking:

An ad hoc network is a peer-to-peer network (no centralized server) that is temporarily set up to be used for some time. For example, a group of employees, each with a laptop or palmtop computer may meet in a conference room for a business or classroom meeting. The employees link their computers in a temporary network only during their meeting.

Figure **1.3** shows the differences between a wireless LAN that supports LAN extension, nomadic access requirements and an ad hoc wireless LAN. In the first case, the wireless LAN forms a stationary infrastructure consisting of one or more cells with a control module for each cell. Within a cell, there may be a number of stationary end systems. Nomadic stations can move from one cell to another. In contrast, there is no infrastructure for an ad hoc network. Rather, a peer collection of stations within range of each other may dynamically configure themselves into a temporary network [1].

1.3 WIRELESS LAN REQUIREMENTS:

A wireless LAN must satisfy all requirements as any wired LAN, such as high capacity, ability to cover short distances, full connectivity among attached stations and broadcast capability. In addition, there are a number of requirements specific to the wireless LAN application. The following are among the most important requirements for a wireless LAN:

Throughput: The MAC (Medium Access Control) protocol should operate very efficiently and use the wireless medium to its maximum capacity.

Number of nodes: A wireless LAN may need to support so many numbers of nodes across multiple cells.

Connection to backbone LAN: To some extent, interconnection with stations on a wired backbone LAN is required. As regards the infrastructure of a wireless LAN, this is simply done by using control modules that connect to both types of LANs. There may also be need for accommodation of mobile users and ad hoc wireless networks.

Service area: The coverage area for a wireless LAN has a diameter of about 100 to 300 m.

Battery power consumption: Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. This indicates that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. In most cases, wireless LAN implementations have features to reduce power consumption while not using the network, such as sleep mode.

Transmission robustness and security: a wireless LAN may be interference-prone and easily eavesdropped. The design of a wireless LAN must provide reliable transmission even in a noisy environment and should permit some level of security from eavesdropping.

Collocated network operation: As wireless LANs become more popular, it is possible for two or more wireless LANs to operate in the same area or in some area where

interference between LANs is possible. This type of interference may disturb the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.

License-free operation: Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

Handoff / roaming: The MAC protocol used in the wireless LAN must provide mobile stations to move from one cell to another.

Dynamic configuration: The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion, and relocation of end system without disruption to other users.

1.4 RESEARCH PROBLREM:

The basic issue addressed in this thesis is to study the behavior and characteristic of a multi cell wireless LAN under different load distributions. This will lead us to compare the current wireless LANs to other types of wired LAN and help in the improvement of existing types of wireless LANs.

1.5 RECENT RESEARCH TRENDS:

In this section we will present a brief survey of some of the resent research work that has been done in related areas to our work, and state their conclusions.

i. Farhan Muhammed Aziz, in his M.Sc. research [3], studies the feasibility and behavior of outdoor implementation of low-cost wireless LANs used for high-mobility telematics and traffic surveillance. A multi-drop experimental wireless data network is designed and tested for this purpose. Outdoor field measurements show the wireless coverage and throughput patterns for static and mobile users. The results suggest the multi-drop wireless LANs can be use for high-mobility application if some protocols are improved.

ii. Srikant Sharma issued a report entitled “Analysis of 802.11b MAC: A QoS, Fairness, and Performance Perspective” [4], he conclude that, despite being widely deployed, 802.11b can not be termed as a well matured technology. Although 802.11b is adequate for basic connectivity issues and packet switching, it is evident that there is ample scope for its improvement in areas like quality of service, fairness, performance, security, .. etc. In his survey report, he identifies and argues that the Medium Access

Controller for 802.11b networks, is the prime area for this improvement. He then proposed a novel scheme called the *Intelligent Collusion Avoidance*, seeking to enhance the MAC to address some of the performance issues in 802.11 and similar networks. The Intelligent Collusion Avoidance tries to improve the channel utilization by allowing the exposed nodes to carry on data transmission in parallel whenever possible. This mechanism leverage in the RTS/CTS messages exchanged during the collusion avoidance phase to deduce the directionality of transmission and RTS/CTS threshold values to carry parallel data transmissions.

iii. Slimane Ben Slimane and Mikael Gidlund issue a paper entitles "Performance of Wireless LANs in Radio Channels" [5]. In this paper they present simulation based results for the channel throughput and normalized packet delay of CSMA/CA MAC protocol operating in the fading channels. They consider an AP located in the center of infrastructure network and mobile stations uniformly distributed over the Basic Service Area (BSA). The radio channel between the AP and the mobile stations is modeled as a Rician fading with constant Rician factor of 10 dB. The average packet delay and the throughput are evaluated for different traffic loads and different of mobile stations. The obtained results show that fading channels reduce the system throughput especially for mobile stations near to cell and create unfairness within the system. They do conclude that the CSMA/CA suffers under the effect of multi-path interference.

1.6 ORGANAZATION OF THE THESIS:

We already had an introduction in chapter one about the Wireless LANs (WLAN).

In Chapter Two a detailed examination is presented of the three principal types of wireless LANs, classified according to transmission technology: infrared, spread spectrum and narrow band microwave. A description is also given of the most prominent specifications for the wireless LAN that was developed by the IEEE 802.11 working group. It includes the overall architecture of the IEEE 802 standards and the specifics of IEEE 802.11.

Chapter Three includes modeling and simulation of a multi cell wireless LAN system, starting with the model for a cellular wireless system and the software for two hosts and five hosts that are sharing wireless transmission media.

Chapter Four describes the results and discussion of the work.

Chapter Five is a conclusion.

Appendix I includes the simulation software and Appendix II includes explanation for some parts of the software.

CHAPTER TWO

Wireless LAN Technology
AND
IEEE 802.11 WIRELESS LAN STANDARDS

2.1 WIRELESS LAN TYPES:

Wireless LANs are categorized into three different categories according to the transmission techniques used in each. These categories are:

Infrared (IR) LANs: Every individual IR LAN cell is limited to a single room due to the inability of infrared light to penetrate opaque walls.

Spread spectrum LANs: These LANs use spread spectrum transmission techniques. They don't require licensing in most cases because they operate in the ISM (Industrial, Scientific, and Medical) bands.

Narrow band microwave LANs: These LANs don't use spread spectrum although they operate in microwave frequencies. While some of these products use one of the unlicensed ISM bands, others operate at frequencies that require FCC (Federal Communications Commission) licensing.

2.1.1 Infrared LANs:

The infrared portion of the spectrum is widely used in most homes, where optical wireless communication is used in a variety of remote control devices. More recently, wireless LANs that use infrared technology have drawn attention. In the next paragraphs a comparison of the characteristics of infrared LANs and those of radio LANs is provided and some of the details of infrared LANs are introduced.

2.1.1.1 Strengths and Weaknesses:

There are two competing transmission medium for wireless LANs: microwave radio that use either spread spectrum or narrow band transmission, or infrared. Infrared techniques offer a number of advantages over the microwave radio transmission. Firstly, extremely high data rates are possible due to the fact that the spectrum is virtually unlimited. This is because the infrared spectrum is unregulated worldwide, which is not the case for some portions of the microwave spectrum. Infrared is attractive for certain types of LAN configurations because it shares some properties of the visible light. For example, ceiling reflection is used to achieve coverage of an entire room, making use of the fact that light-colored objects diffusely reflect infrared light. The fact that infrared

light does not penetrate opaque walls or other objects has two advantages: Firstly, infrared communication can be more easily secured against eavesdropping than microwaves; and secondly, a separate infrared installation can operate in every room in a building without interference, thus enabling the construction of very large infrared LANs. The strength of using infrared LANs is the fact that the equipment is relatively inexpensive and simple. Intensity modulation is used in infrared data transmission, so that while most microwave receivers must detect phase or frequency, IR receivers need only to detect amplitude of optical signals.

There are some disadvantages for using infrared medium. Sunlight and indoor lighting cause intense ambient infrared background radiation in indoor environments, which appears as noise in infrared receivers. This requires the use of higher power transmitters in addition to limiting the range. Also, concerns of eye safety and consumption of power limit the increase of transmitted power.

2.1.2 Spread Spectrum LANs:

Spread spectrum techniques are currently the most popular type of wireless LANs. Spread spectrum wireless LANs in most cases make use of a multiple-cell arrangement, except for small offices. In order to avoid interference, adjacent cells use different center frequencies within the same band.

In a given cell, the topology can be either hub or peer-to-peer. In a hub topology (Figure 1.2), the hub is usually mounted on the ceiling and connected to a backbone wired LAN to provide connectivity to stations linked to it and to stations, which are part of other wireless LANs in other cells. In addition, the hub can also control access, as in the IEEE 802.11 point coordination function. The hub may also act as a multi-port repeater with similar functionality to the multi-port repeaters of 10Mbps and 100 Mbps Ethernet, thus being able to control access. In this case, all stations in a cell transmit and receive only to and from the hub. On the other hand, and regardless of the access control mechanism, a logical bus configuration may be achieved when each station broadcasts using an omni-directional antenna that all other stations in the cell may receive.

Another potential function of a hub is automatic handoff of mobile stations. Stations are dynamically assigned to a given hub based on proximity, but when the hub senses a weakening signal, it can automatically hand off to the nearest adjacent hub.

A peer-to-peer topology is one in which there is no hub. A MAC algorithm such as carrier-sense multiple access (CSMA) is used to control access. This topology is appropriate for ad hoc LANs [1].

2.1.2.1 Transmission Issues:

Licensing regulations differ from one country to another, and in some cases the use of wireless LANs does not need any licensing procedure. However, as an example in the United States of America, the use of spread spectrum wireless LANs in the ISM band has become popular since the FCC authorized the unlicensed use of it for two applications, spread spectrum and very low power systems.

Of the bands that are used for unlicensed spread spectrum transmission the 2.4-2.4835GHz (2.4-GHz band) is used in the US, Europe, and Japan. Interference with devices that work in this band should be considered. A typical spread spectrum wireless LAN was limited to just 1 to 3 Mbps [1].

2.1.3 Narrow Band Microwave LANs:

In narrow band microwave transmission, microwave radio signals are transmitted in a relatively narrow bandwidth that is wide enough only to accommodate the signal. Most narrow band microwave LAN products use licensed bands, whereas recently some started operating in the ISM band.

2.2 IEEE 802 ARCHITECTURE:

The layerings of protocols that manage the basic functions of a LAN are used to describe the architecture of a LAN. First, we describe the standardized protocol architecture for LANs, which includes physical, medium access control, and logical link control layers. Furthermore we look in more detail at the medium access control and logical link control.

2.2.1 Protocol Architecture:

The protocols, defined specifically for LAN and MAN (Metropolitan Area Network) transmission, concern the transmission of blocks of data over the networks. In OSI (Open System Interconnection) terms, higher-layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs, MANs, and WANs

(Wide Area Network). Thus, a discussion of LAN protocols is concerned principally with lower layers of the OSI model [1].

Figure 2.1 shows the LAN protocols compared to the OSI architecture. This architecture was defined by the IEEE 802 committee and has been adopted by all organizations on the specifications of LAN standards. It is known as the IEEE 802 reference model.

The lowest layer of the IEEE 802 reference model corresponds to the physical layer of the OSI model and includes such functions as:

- Encoding/decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/reception

The physical layer of the 802 models includes a specification of the transmission medium and the topology. However, this is considered “below” the lowest layer of the OSI model. Since the selection of transmission medium and topology is critical in LAN design, a specification of the medium is included.

Above the physical layer are functions associated with providing service to LAN users. These include the following:

- On transmission, assemble data into a frame with address and error detection fields.

- On reception, disassemble frame, and perform address recognition and error detection.
- Govern access to the LAN transmission medium.
- Provide an interface to a higher layer and perform flow and error control.

These functions correspond to those in OSI layer 2. The set of functions in the last line are grouped into a logical link control (LLC) layer. The functions in the first three lines are treated as a separate layer, called medium access control (MAC). The separation is done for the following reasons:

- The logic required to manage access to share-access medium is not found in traditional layer 2 data link control.
- For the same LLC, several MAC options may be provided.

Figure 2.2 illustrates the relationship between the levels of the architecture. Higher level data are passed down to LLC, which appends control information as a header, creating an LLC protocol data unit (PDU). This control information is used in the operation of LLC protocol. The entire LLC/ PDU is then passed down to the MAC layer, which appends control information at the front and back of the packet, forming a MAC frame. Again, the control information in the frame is needed for the operation of the MAC protocol. For context, the figure also shows the use of TCP/IP and an application layer above the LAN protocols.

2.2.2 MAC Frame Format:

The MAC sub-layer receives the data from the LLC sub-layer. The MAC layer is responsible for performing functions related to medium access and passing the data to the upper layers. The MAC uses PDU at its layer to implement its functions. The PDU is referred to as a MAC frame. The MAC frame has a format similar to that shown in **Figure 2.3**. The fields of this frame are as follows:

- **MAC control**: This includes any protocol control information required for the functioning of the MAC protocol. For example, a priority level could be indicated here.
- **Destination MAC address**: The destination physical attachment point on the LAN for this frame.
- **Source MAC address**: The source physical attachment point on the LAN for this frame.
- **Data**: The body of the MAC frame. This may be LLC data from the next higher layer or control information relevant to the operation of the MAC protocol.
- **CRC**: The CRC (cyclic redundancy check) field, also known as the frame check sequence (FCS) field. This is an error-detection code.

Usually the entity of the data link control protocols is responsible for detecting errors using the CRC and correcting generated errors by retransmitting damaged frames. In the LAN protocol

architecture, these two functions are split between the MAC and LLC layers. The MAC layer is responsible for detecting errors and discarding any frames that are in error. The LLC layer ensures that frames have been successfully received and retransmits unsuccessful frames.

2.2.3 Logical Link Control (LLC):

The LLC layer transmits a link- level PDU between two stations, without an intermediate switching node. The LLC has two characteristics that are not found in other link control protocols:

1. It must support the multi-access, shared-medium nature of the link (this differs from a multi-drop line in that there is no primary node).
2. It is relieved of some details of link access by the MAC layer.

Addressing in LLC involves specifying the source and destination of LLC users. A user is a higher-layer protocol or a network management functions in the station. These LLC user addresses are referred to as service access points SAPs (Service Access Points).

2.2.3.1 LLC Services:

The LLC handles addressing of stations across the medium and controls the exchange of data between two users. The operation and format of this standard is based on HDLC (High-Level Data Link Control). Three services are provided as alternatives for attached devices using LLC:

Unacknowledged connectionless service: This service is a datagram-style service. It is a very simple service that does not involve any of the flow-and-error control mechanisms. Thus, the delivery of data is not guaranteed. However, in most devices, there will be some higher layer of software that deals with reliability issues.

Connection-mode service: This service is similar to that offered by HDLC. A logical connection is set up between two users exchanging data, and flow control and error control are provided.

Acknowledged connectionless service: This is a cross between the previous two services. It provides that datagrams are to be acknowledged, but no prior logical connection is set up.

2.2.3.2 LLC Protocol:

The basic LLC protocol is modeled after HDLC and has similar functions and formats. The differences between the two protocols can be summarized as follows:

- LLC makes use of the asynchronous balanced mode of the operation of HDLC, to support connection-mode LLC service; this is referred to as type 2 operation. The other HDLC modes are not employed.
- LLC supports an unacknowledged connectionless service using the un-numbered information PDU; this is known as type 1 operation.
- LLC supports an acknowledged connectionless service by using two new un-numbered PDU; this is known as type 3 operation.
- LLC permits multiplexing by the use of LLC service access points (LSAPs).

All three LLC protocols employ the same PDU format (**Figure 2.3**), which consists of four fields. The DSAP and SSAP fields contain 7-bits address each, which specify the destination and source users of LLC. One bit of the DSAP indicates whether the DSAP is individual or group address. One bit of the SSAP indicates whether the PDU is a command or response PDU.

For type 1 operation, which supports the unacknowledged connectionless service, the un-numbered information (UI) PDU is used to transfer user data. There is no acknowledgement, flow control, or error control. However, there is error detection and discard at the MAC level.

Two other PDU types, XID and TEST, are used to support management functions associated with all three types of operation. Both PDU types are used in the following fashion. An LLC entity may issue a command (C/R bit=0) XID or TEST. The receiving LLC entity issues a corresponding XID or TEST in response. The XID PDU is used to

exchange two types of information: types of operations supported and window size. The TEST PDU is used to conduct a loop back test of the transmission path between two LLC entities. Upon receipt of a TEST command PDU, the addressed LLC entity issues a TEST response PDU as soon as possible.

With type 2 operation, a data link connection is established between two LLC SAPs prior to data exchange. Connection establishment is attempted by type 2 protocol in response to a request from a user. The LLC entity issues a SAMBME PDU to request a logical connection with the other LLC entity. If the connection is accepted by the LLC user designated by the DSAP, then the destination LLC entity returns an un-numbered acknowledgement (UA) PDU. The connection is henceforth uniquely identified by the pair of user SAPs. If the destination LLC user rejects the connection request, its LLC entity returns a disconnected mode (DM) PDU.

Once the connection is established, data is exchanged using information PDUs, as in HDLC. The information PDUs include send and receive sequence numbers, for sequencing and flow control. The supervisory PDUs are used, as in HDLC, for flow control and error control. Either LLC entity can terminate a logical LLC connection by issuing a disconnect (DISC) PDU.

With type 3 operation, each transmitted PDU is acknowledged. A new (not found in HDLC) un-numbered PDU, the acknowledged connectionless (AC) information PDU, is defined. User data are sent in AC command PDUs and must be acknowledged using an AC response PDU. To guard against lost PDUs, a 1-bit sequence number is used. The sender alternates the use of 0 and 1 in the AC command PDU, and the receiver responds with an AC PDU with the opposite number of the corresponding command. Only one PDU in each direction may be outstanding at any time.

2.3 IEEE 802.11 ARCHITECTURE AND SERVICES:

Work on wireless LANs within the IEEE 802 committee began in 1987 with the IEEE 802.4 group. It was developed as an ISM-based wireless LAN using the equivalent of token-passing bus MAC protocol. Later on, it was noticed that token bus was not suitable for controlling a radio

medium without causing inefficient use of the radio frequency spectrum. IEEE 802 then decided in 1990 to form a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification. **Table 2.1** briefly defines key terms used in the IEEE 802.11 standard.

2.3.1 IEEE 802.11 Architecture:

Figure 2.4 illustrates the model of the 802.11 working group. The smallest unit block of a wireless LAN is a basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium. A BSS may be isolated or it may be connected to a backbone distribution system (DS) through an access point (AP). The access point functions as a bridge. The MAC protocol may be fully distributed or controlled by a central coordination function housed in the access point. The BSS generally corresponds to what is referred to as a cell in the literature. The DS can be a switch, a wired network, or a wireless network [1].

The simplest configuration is shown in Figure 2.4**,** in which each station belongs to a single BSS, and will be within wireless range only of other stations within the same BSS. It is also possible for two BSSs to overlap geographically, so that a single station could operate in more than one BSS. An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system. The extended service set appears as a single logical LAN to the logical link control (LLC) level.

Also, Figure 2.4 indicates that an access point (AP) is implemented as part of a station; the AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a portal is used. The portal is implemented in a device, such as a bridge or router that is part of the wired LAN, which is attached to the DS.

2.3.2 IEEE 802.11 Services:

IEEE 802.11 defines nine services that need to be offered by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs. There are two ways of categorizing the services:

1. The service provider can be either the station or the distribution system (DS). Station services are implemented in every 802.11 station, including

access point (AP) stations. Distribution services are provided between basic service sets (BSS); these services may be implemented in an AP or in another special-purpose device attached to the distribution system.

2. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Six of the services are used to support delivery of MAC service data units (MSDUs) between stations. The MSDU is the block of data passed down from

the MAC user to the MAC layer. Typically this is an LLC PDU. If the MSDU is too large to be transmitted in a single MAC frame, it may be fragmented and transmitted in a series of MAC frames.

2.3.2.1 Access and Privacy Services:

There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, in that it requires some positive and presumably observable action to connect a station to a wired LAN.
2. Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station must be also attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range

can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

IEEE defines three services that provide a wireless LAN with these two features:

- **Authentication**: Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN, in which connectivity is achieved simply by having an attached antenna that is properly tuned. The authentication service is used by stations to establish their identity with stations they wish to communicate with. IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality scheme. IEEE 802.11 requires successful authentication before a station can establish an association with an AP.
- **Deauthentication**: This service is invoked whenever an existing authentication is to be terminated.
- **Privacy**: This is used to prevent the contents of a message from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy. The algorithm specified in the standard is WEP (Wired Equivalent Protocol).

2.4 IEEE 802.11 MEDIUM ACCESS CONTROL (MAC):

The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security.

2.4.1 Reliable Data Delivery:

A wireless LAN using the IEEE 802.11 physical and MAC layers is having some sort of unreliability. Noise, interference, and other propagation effects result in a loss of a number of frames. Even with error-correction codes, a number of MAC frames may not successfully be received. This situation can be dealt with by reliability mechanisms at higher layers, such as TCP. It is therefore more efficient to deal with errors at the MAC level. For this purpose, IEEE 802.11 includes a frame exchange protocol. When a station

receives a data frame from another station it returns an acknowledgement (ACK) frame to the source station. This exchange is having higher priority and must not be interrupted by a transmission of any other station. If the source does not receive an ACK within a short period of time, either because its data frame was damaged or because the returning ACK was damaged, the source retransmits the frame.

Thus, the basic data transfer mechanism in IEEE 802.11 involves an exchange of two frames. To further enhance reliability, a four-frame exchange may be used. In this scheme, a source first issues a request to send (RTS) frame to the destination. The destination then responds with a clear to send (CTS). After receiving the CTS, the source transmits the data frame, and the destination responds with an ACK. The RTS alerts all stations that within reception range of the source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time. Similarly, the CTS alert all stations that are within reception range of the destination that an exchange is under way.

2.4.2 Access Control:

The 802.11 working group considered two types of proposals for a MAC algorithm: Distributed access protocols, which distribute the decision to transmit over all nodes using carrier sense mechanism; and centralized access protocols, which involves regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad hoc network of peer workstations and may also be attractive in other wireless LAN configurations that consist primarily of bursting traffic. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to backbone wired LAN; it is especially useful if some of the data is time sensitive or high priority.

The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. **Figure 2.5** illustrates the architecture. The lower sub-layer of the MAC layer is the distribution coordination function (DCF). The DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF. The point coordination function (PCF) is a centralized MAC

algorithm used to provide contention-free service. The PCF is built on top of DCF and exploits features of DCF to assure access for its users [1].

2.4.2.1 Distributed Coordination Function

The DCF sub-layer makes use of a simple CSMA (carrier sense multiple access) algorithm. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit, otherwise the station must wait until the current transmission is complete before transmitting. The DCF does not include a collision detection function (i.e., CSMA/CD) because collision detection is not practical on a wireless network. The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

DCF includes a set of delays that amounts to a priority scheme. Let us start by considering a single delay known as an inter-frame space (IFS). Using IFS, the rules for CSMA access are as follows:

1. A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
2. If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.
3. Once the current transmission is over, the station delays other IFS. If the medium remains idle for this period, then the station backs off a random amount of time

and again sense the medium. If the medium is still idle, the station may transmit. During the back-off time, if the medium becomes busy, the back-off timer is halted and resumes when the medium becomes idle.

To ensure that back-off maintains stability, a technique known as binary exponential back-off is used. A station will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled. The Binary exponential back-off (BEB) provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer back-off times, which helps to smooth out the load. Without such a back-off, the following situation could occur. Two or more stations attempt to transmit at the same time, causing a new collision.

The Preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS:

- SIFS (short IFS): The shortest IFS, used for all immediate response actions, as explained in the following discussion
- PIFS (point coordination function IFS): A mid-length IFS, used by the centralized controller in the PCF scheme when issuing polls.
- DIFS (distributed coordination function IFS): The longest IFS, used as a minimum delay for asynchronous frames contention for access

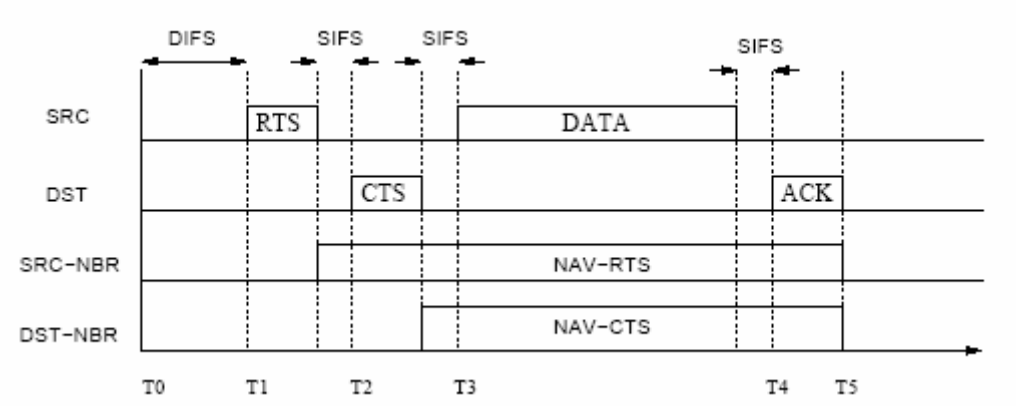

Figure 2.6 Message exchanges in DCF [5].

Figure 2.6 illustrates the scenario of the 4-way hand shake [3]. Each DATA packet is preceded by a RTS and a CTS messages. On hearing RTS, the nodes in vicinity of

senders set their Network allocation vectors (NAVs) to the duration mentioned by RTS. On hearing CTS, the nodes in the vicinity of receiver set their NAVs to the duration mentioned in the CTS. This causes in establishment of the channel reservation till the time the ACK is sent back to the sender. Also Figure 2.7 shows the use of IF time values. Consider first the SIFS. Any station using SIFS to determine transmission opportunity has, in effect the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS. The SIFS is used in the following circumstances:

- Acknowledgement (ACK): When a station receives a frame addressed only to itself (not multicast or broadcast) it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC protocol data unit (PDU) that requires multiple MAC frames. In this case, the following scenario occurs. A station with multiframe LLC PDU to transmit sends out the MAC frames one at a time. The recipient acknowledges each frame after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.
- Clear to Send (CTS): A station can ensure that its data frame will get through by first issuing a small Request to Send (RTS) frame. The station to which this frame is addressed should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.
- Poll response: This is explained in the following discussion of PCF.

The next longest IFS interval is the PIFS. This is used by the centralized controller in issuing polls and takes precedence over normal contention traffic. However, those frames transmitted using SIFS have precedence over a PCF poll.

Finally, the DIFS interval is used for all ordinary asynchronous traffic.

2.4.2.2 Point Coordination Function:

PCF is an alternative access method implemented on top of the DCF. The operation consists of polling by the centralized polling master (point coordinator). The point coordinator makes use of PIFS when issuing polls. Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses.

As an extreme, consider the following possible scenario. A wireless network is configured so that the point coordinator (PC) controls a number of stations with time-sensitive traffic while remaining traffic contends for access using CSMA. The point coordinator could issue polls in a round-robin fashion to all stations configured for polling. When a poll is issued, the polled station may respond using SIFS. If the point coordinator receives a response, it issues another poll using PIFS. If no response is received during the expected turnaround time, the coordinator issues a poll.

If the discipline of the preceding paragraph were implemented, the point coordinator would lock out all asynchronous traffic by repeatedly issuing polls. To prevent this, an interval known as the super frame is defined. During the first part of this interval, the point coordinator issues polls in a round-robin fashion to all stations configured for polling. The point coordinator then idles the reminder of the super frame, allowing a contention period for asynchronous access.

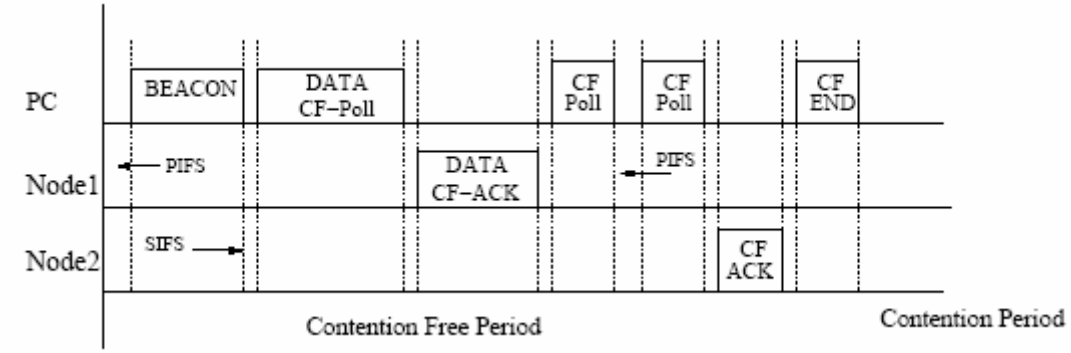

Figure 2.7 A super frame in IEEE 802.11b [5]

Figure 2.7 illustrates the use of the super frame [3]. At the beginning of a super frame, the point coordinator may optionally seize control and issues polls for a given period of time. This interval varies because of the variable frame size issued by responding stations. The reminder of the super frame is available for contention-based access. At the end of the

super frame interval, the point coordinator contends for access to the medium using PIFS. If the medium is idle, the point coordinator gains immediate access and a full super frame period follows. However, the medium may be busy at the end of a super frame. In this case, the point coordinator must wait until the medium is idle to gain access; this result in a foreshortened super frame period for the next cycle**.**

2.4.3 MAC Frame:

Figure 2.8a illustrates the 802.11 frame format. This general format is used for all data and control frames, but not all fields are used in every context. The fields are as follows:

- **Frame control**: indicates the type of frame and provides control information.
- **Duration/connection ID**: if used as a duration field, indicates the time (in microseconds) that the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association or connection identifier.
- **Addresses**: the number and meaning of the address fields depend on context. Address types include source, destination, transmitting station, and receiving station.
- **Sequence control**: contains a 4-bit fragment number subfield, used for fragmentation and re-assembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- **Frame body**: contains an MSDU or a fragment of an MSDU. The MSDU is an LLC protocol data unit or MACV control information.
- **Frame check sequence**: a 32-bit cyclic redundancy check.

The frame control field, shown in **Figure 2.8b**, consists of the following fields:

- **Protocol version**: 802.11 version, currently version 0
- **Type**: identifies the frame as control, management, or data.
- **Subtype**: further identifies the function of frame. **Table 2.1** defines the valid combination of type and subtype.

- **To DS**: the MAC coordination sets this bit to 1 in a frame destined to the distribution system
- **From DS**: the MAC coordination sets this bit to 1 in a frame leaving the distribution system.
- **More fragments**: set to 1 if more fragments follow this one.
- **Retry**: set to 1 if this is a retransmission of a previous frame
- **Power management**: set to 1 if the transmitting station is in a sleep mode.
- **More data**: indicates that a station has additional data to send. Each block of data may be sent as one frame or a group of fragments in multiple frames.
- **WEP**: set to 1 if the optional wired equivalent protocol is implemented. WEP is used in the exchange of encryption keys for secure data exchange.

- **Order**: set to 1 in any data frame sent using the Strictly Ordered service, which tells the receiving station that the frame must be processed in order.

2.4.3.1 Control Frames:

Control frames improve the delivery of data frames. There are six control frame subtypes:

- **Power save-poll (PS-Poll)**: This frame is sent by all stations to the station that includes the AP (access point). Its purpose is to request that the AP transmits a frame that has been buffered for this station while the station was in the power-saving mode.
- **Request to Send (RTS)**: This frame is the first frame in the four-way frame exchange discussed under the subsection on reliable data delivery. The station sending this message is alerting a potential destination, and all

other stations within the reception range that it intends to send a data frame to that destination.

- **Clear to Send (CTS)**: This is the second frame in the four-way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
- **Acknowledgement**: Provides an acknowledgement from the destination to the source that the immediately preceding data, management, or PS-Poll frame was received correctly.
- **Contention-free (CF)-end**: Announces the end of a contention-free period that is part of the point coordination function.
- **CF-end + CF-ack**: Acknowledges the CF-end. This frame ends the contention-free period and releases stations from the restriction associated with that period.

2.4.3.2 Data Frames:

There are eight data frames subtypes, organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames are as follows:

- **Data**: This is the simplest data frame. It may be used in both a contention period and a contention-free period.
- **Data + CF-Ack**: May only be sent during a contention-free period. In addition to carrying data, this frame acknowledges previously received data.
- **Data + CF-Poll**: Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
- **Data + CF-Ack + CF-Poll**: Combines the functions of the Data + CF-Ack and Data + CF-Poll into a single frame.

The remaining four subtypes do not in fact carry any user data. The Null Function data frame carries no data, polls, or acknowledgement. It is used only to carry the power management bit in the frame control field to the AP, to indicate that the station is changing to low power operating state. The remaining three

frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) have the same functionality as the corresponding data subtypes in the preceding list but without the data.

2.4.3.3 Management Frames:

Management frames are used to manage communication between stations and APs. The following subtypes are included:

- **Association request**: Sent by a station to an AP to request an association with the BSS. This frame includes capability information, such as whether encryption is to be used and whether this station is pollable.
- **Association response**: Returned by the AP to the station to indicate whether it is accepting this association request.
- **Reassociation request**: Sent by a station when it moves from one BSS to another and needs to make an association with the AP in the new BSS. The station uses re-association rather than simply association, so that the new AP knows to negotiate with the old AP for the forwarding of data frames.
- **Reassociation response**: Retuned by the AP to the station to indicate whether it is accepting this reassociation request.
- **Probe Request**: Used by a station to obtain information from another station or AP. This frame is used to locate an IEEE 80211 BSS.
- **Probe response**: Response to a probe request.
- **Beacon**: Transmitted periodically to allow mobile stations to locate and identity a BSS.
- **Announcement traffic indication message**: Sent by a mobile station to alert other mobile stations that may have been in a low power mode that this station has frames buffered and is waiting to be delivered to the station addressed in this frame.
- **Dissociation**: Used by a station to terminate an association.
- **Authentication:** Multiple authentication frames are used in an exchange to authenticate one station to another.
- **Deauthentication:** Sent by a station to another station or AP to indicate that it is terminating secure communication.

2.4.4 Security Considerations:

IEEE 802.11 provides both privacy and authentication mechanisms.

The wired equivalent privacy algorithm:

With a wireless LAN, eavesdropping is a major concern because of the ease of capturing a transmission. IEEE 802.11 incorporates WEP to provide a modest level of security. To provide privacy, as well as data integrity, WEP uses an encryption algorithm based on the RC4 encryption algorithm.

Figure 2.9a shows the encryption process. The integrity algorithm is simply the 32-bit CRC that is appended to the end of the MAC frame. For the encryption process, the two participants in the exchange share a 40-bit secret key. An initialization vector (IV) is concatenated to the secret key. The resulting block forms the seed that is input to the pseudorandom number generator (PRNG) defined in RC4. The PRNG generates a bit sequence of the same length as the MAC frame plus its CRC. A bit-by-bit exclusive-OR between the MAC frame and the PRNG sequence produces the cipher text. The IV is attached to the cipher text and the resulting block is transmitted. The IV is changed periodically. Every time the IV is changed, the PRNG sequence is changed, which complicates the task of an eavesdropper.

At the receiving end (**Figure 2.9b**), the receiver retrieves the IV from the data block and concatenates this with the shared secret key to generate the same key sequence used by the sender. This key sequence is then XOR-ed with the incoming block to recover the plaintext.

Finally, the receiver compares the incoming CRC with the CRC calculated at the receiver to validate integrity:

1. A transmits an authentication frame that includes the challenge text just received from B. The entire frame is encrypted using WEP.
2. B receives the encrypted frame and decrypts it using WEP and the secret key shared with A. If decryption is successful (matching CRCs), then B compares the incoming challenge text with the challenge text that it sent in the second message. B then sends an authentication message to A with a status code indicating success or failure.

2.5 IEEE 802.11 PHYSICAL LAYER:

The physical layer for IEEE 802.11 has been issued in three stages; the first part was issued in 1997 and the remaining two parts in 1999. The fist part, simply called IEEE 802.11, includes the MAC layer and three physical layer specification, two in the 2.4-GHz band and one in the infrared, all operating at 1 and 2 Mbps. IEEE 802.11a operates in the 5-GHz band at data rate up to 54 Mbps. IEEE 802.11b operates in the 2.4-GHZ band at 5.5 and 11 Mbps.

Original IEEE 802.11 Physical Layer

Three physical layer are defined in the original 802.11 standard:

- Direct sequence spread spectrum operating in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps.
- Frequency hopping spread spectrum operating in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps.
- Infrared at 1 Mbps and 2 Mbps operating at wavelength between 850 and 950 nm

2.5.1 Direct Sequence Spread Spectrum (DS-SS):

Up to even channels, each with a data rate of 1 Mbps or 2 Mbps can be used in the DS-SS system. The number of channels available depends on the bandwidth allocated by the various national regulatory agencies. Each channel has a bandwidth of 5 Mhz. The encoding scheme that is used is DBPSK for the 1-Mbps rates and DQPSK for the 2-Mbps rates. For IEEE 802.11, a Barker sequence is used.

2.5.2 Frequency-Hopping Spread Spectrum (FH-SS):

FH-SS system makes use of a multiple channels, with the signal hopping from one channel to another based on pseudo-noise sequence. In the case of the IEEE 802.11 scheme, 1-MHz channel are used.

For modulation, the FH-SS scheme uses two-level Gaussian FSK for the 1-Mbps system. The bit zero and one are encoded as deviation from the current carrier frequency. For 2-Mbps, a four-level GFSK scheme is used, in which four different deviations from the center frequency define the four 2-bit combinations.

2.5.3 Infrared:

The IEEE 802.11 infrared scheme is omni-directional rather than point-to-point system. A range of up to 20 m is possible. The modulation scheme for the 1-Mbps data rate is known as 16-PPM (pulse position modulation). In this scheme, each four group of 4 data bits is mapped into one of the 16-PPM symbols; each symbol is a string of 16 bits. Each 16 bit string consists of fifteen 0s and one binary 1. For the 2-Mbps data rate, each group of 2 data bits is mapped into one of the four 4-bit sequences. Each sequence consists of three 0s and one binary 1. The actual transmission uses an intensity modulation scheme, in which the presence of a signal corresponds to a binary 1 and the absence of a signal corresponds to binary 0.

2.5.4 IEEE 802.11a:

The IEEE 802.11a specification makes use of the 5-GHz band. Unlike the 2.4-GHz specification, IEEE 802.11 does not use a spread spectrum scheme but rather uses orthogonal frequency division multiplexing (OFDM). However, in the case of OFDM, all the subchannels are dedicated to a single data source.

The possible data rates for IEEE 802.11a are 6, 9, 12, 18, 24, 36, 48, and 54Mbps. The system uses up to 52 subcarriers that are modulated using BPSK, QPSK, 16-QAM, or 64-QAM, depending on the rate required. Subcarrier frequency spacing is 0.3125 MHz. A convolutional code at rate of ½, 2/3, or ¾ provides forward error correction.

2.5.5 IEEE 802.11b:

IEEE 802.11b is an extension of the IEEE 802.11 DS-SS scheme, providing data rates of 5.5 and 11 Mbps. The chipping rate is 11 MHz, which is the same as the original DS-SS scheme, thus providing the same occupied bandwidth. To achieve a higher data rate in the same bandwidth at the same chipping rate, a modulation scheme known as complementary code keying (CCK) is used.

The CCK modulation scheme is quite complex. Input data are treated in blocks of 8 bits at a rate of 1.375 MHz. Six of these bits are mapped into one of 64- codes sequences based on the use of the 8 x 8 Walsh matrixes. The output of the mapping, plus the two additional bits, forms the input to a QPSK modulator.

CHAPTER THREE

MODELING & SIMULATION OF A MULTI CELL WIRELESS LAN

3.1 MODELING OF A MULTI CELL WIRELESS LAN:

The simulation for multi cells wireless LAN describes and investigates both its behavior and its performance. This simulation is based on a proposed model of a wireless

LAN. The proposed model is based on some assumptions that emerged from the standard of the wireless LAN. The model may be described as follows:

- There are a number of hosts at fixed positions distributed within the coverage area.
- Each of these hosts represents an access point AP and belongs to different Basic service set BBS (cells) at a clear line of site LOS. They send their packets directly to each others.
- The noise, fading and other atmospheric affects introduce residual errors and lead to retransmission of packets.
- Each host has a finite buffer.
- The decision to send a message follows the Poisson law [2]:

$$P_n(t) = (\lambda t)^n . e^{-\lambda t}/n! \quad \text{.....(3.1)}$$

Where, $P_n(t)$: Probability that a message arrive during interval t.

n = number of messages arriving during time interval of length t

λ = mean arrival rate.

t = time

- From the above assumption one may assume the following:
    1. Inter-arrival times of a message are exponentially distributed.
    2. The message duration is exponentially distributed.

  For both the inter-arrival time and the message duration the power density function is:

$$p(\tau) = \lambda e^{-\lambda \tau} \quad \text{.....(3.2)}$$

where,

λ = probability density function constant, mean inter-arrival rate

τ = time

By integrating both sides we get:

$P(\tau) = 1-e^{-\lambda\tau}$ …… (3.3)

From which the inter-arrival time or message duration time can be determined in two steps:

a. Generate a uniform random variable number $u = P(\tau)$ in the range (0,1)

b. Inter-arrival or message duration time from equation (5.3):

$\tau = - \ln (1-u) /\lambda$ …… (3.4)

The average inter-arrival time and average message duration time may be calculated as follows:

$$\tau' = \int \tau.p(\tau)d\tau.$$
$$= \int \tau. \lambda e^{-\lambda\tau} d\tau.$$
$$= 1/\lambda = \lambda'$$

- Each host completes sending the message before it decides to send another.
- The message is constructed from packets and the packets will be sent according to the CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) protocol.
- The time for sending the message varies from one message to another.
- The packets are correlated.
- Residual errors are introduced in the transmission channel due to noise and other atmospheric affects.
- The hosts are distributed within the coverage area.

3.3 THE SIMULATION SOFTWARE FOR FIVE HOSTS:

The code for the program is written in C++ language. In this simulation five hosts are sharing the wireless transmission media. It is assumed that they are distributed within the coverage area of the wireless LAN network. The Carrier Sense Multiple Access/Collision Avoidance protocol (CSMA/CA) is used to manage their transmission. Also noise and other atmospheric effects affect the transmission media, and therefore some residual errors are introduced during the transmission of the packets. In the program errors are added to the packets string randomly and the lost packets are retransmitted again.

The flow chart of the program is shown in the following diagram. The program begins by defining some values. PERR is the probability that an error may occur for the characters of the packet string. It is a percentage from a random number between (1 to 100) divided over a fixed value.

The function send is used to randomly generate a string that will be transmitted in the transmission channel. Also it add according to a random condition an errors to the transmitted string. The send function returns the number of re-transmissions of the packet.

Some functions are defined to calculate the message duration (exponentially distributed) for the message arriving at the hosts. The mean arrival rate for the messages is fixed for all hosts and the user enters it. Also the function inter-arrival is used to generate the inter-arrival times (exponentially distributed) for the received message at the hosts. The mean inter arrival rates lamda (load) varies with time with an incremental value . Another function is used for the generation of a random delay time in the range (0.0 to 1.0) unit of time.

Next the main function, which is the body of the simulation program begins.

The variables are declared and initialized and the user enters the simulation time and both mean arrival and inter-arrival rates.

The frame length of the packet is assigned, and also the bit rate is selected. From these values the packet duration is calculated.

Next a do – while loop begins, every time it checks the condition that the counter of the total time is less than the given simulation period of the program.

Inside the loop there are five consecutively if conditional blocks, to be performed for each of the five hosts. The if block statements are executed whenever the value of the packet number is less than or equal to zero. The following tasks are performed:

1. Generation of inter arrival time for a new message.
2. Updating the counter of the inter-arrival time.
3. Generation of message duration for the new message.
4. Increment the value of lamda (mean inter-arrival rate).
5. Calculate the number of packets for the new message.
6. Increment the counter of the number of messages.

These IF blocks will be all executed in the first time, for the generation of the first message at all hosts. The corresponding block will be executed for a host, when the host has finished sending all the packets of the previous message.

Next there is an ELSE IF nested conditional structure consisting of the following:

1) First (if), the case that all the inter arrival times of the hosts are equals, that is each the host is having a message ready to be send at the same instant of time. If this is true, a random time is added to all inter arrival times, and starts the do loop again.

2) Second (else if), the inter arrival time of host 1 is less than or equal to any of the inter-arrival times of the other four hosts. When this is the case:

Another (if conditional), to check whether the inter-arrival time of host 1 individually equal to any of the inter- arrival times of the other four hosts, and add a random time to the match case. If the condition remains true, the following tasks are performed:

i. The total time counter is adjusted
ii. The message duration counter of host 1 is incremented

iii. The function send is called, packet is sent and the number of retransmission is returns by the function send. It is assumed that host 1 sent first request to send (RTS) and received a clear to send CTS message from the destination before attending to sent its message packets, therefore the transmission media is idle during the transmission instant and all other host will not attempt to send after listening to the CTS message to host 1, when the packet sent by host 1 is transmitted successfully, host 1 receives an acknowledge message from the destination.

iv. Delay is incremented if the packet retransmitted again

v. Total counter time is incremented

vi. Inter arrival time is incremented by the value of the packet duration

vii. The number of packet is decreased

viii. The number of successfully transmitted packet incremented

ix. The message number and the packet number sent by host1 are printed.

x. The total time at this moment is printed

3) Third (else if), the inter arrival time of host 2 is less than or equal to any of the enter arrival times of the remaining three host. If this is the case, the same procedure treated for host 1 will follow for host 2.

4) Fourth (else if), the inter arrival time of host 3 is less than or equal to those of host4 or host 5. The same concept applied as done above for host 1

5) Fifth (else if), the inter arrival time of host 4 is less than or equal to that of host 5. Again the same procedure is done.

6) Last (else), for host 5, and it follows the same manner as done for host 1.

The nested else if conditional structure manages the process of sending the packets of the message generated for the hosts during the simulation portion of time.

Then the utilization of the hosts to the wireless transmission media is calculated for each host, and throughput of the transmission channel is determined. Since the load varies (mean inter arrival rate) with time, the behavior of the wireless LAN can be studied during the portion of the simulation time.

When the do-while loop condition is verified, the simulation process is terminated, and the values of the throughputs are printed.

CHAPTER FOUR

RESULTS AND DISCUSSION

We refer first to the results and samples of output of the simulation program for five hosts, which is our essential simulation that satisfy the points of the model mentioned at section 3.1 of chapter three. There are two forms of print sheets of output by hiding some of the print syntax output ward “cout” . Let us examine and discuss the first type in which the output printed sheet contains the following (The output result carves are attached in the appendix):

Values entered by the user, which are:

i. The given simulation period (any random units of time).
ii. The mean inter arrival rate of the message at the hosts (constant value).
iii. The mean arrival rate of the message duration (constant value).

The output result of the software in which we obtain the following:

i. The arriving time of the first message at all hosts and their corresponding message durations time units.
ii. The successfully sent packet from a message of a host, and the total time at this moment of time during the simulation period of the software.
iii. The number of transmission times of a packet.
iv. The corresponding number of the transmission and retransmission times if any in the channel.
v. The utilization of the hosts to the transmission channel.
vi. The total utilization of the transmission media.

The above samples results shown in the output sheet were obtained at fixed constant value of lamda (load) during the simulation portion. Other parameters or data are investigated and observed their effect in the other sort of output sheets,

and also they are fixed during the execution of the program at these moments.
Looking again in deep one may realize the following:
The overall throughput is slightly above half of the full utilization of the wireless LAN transmission media. Also the number of retransmission times varies, and this takes very short period of time. Each retransmission tray add a delay equal to the packet duration time to all hosts. We are not sure this number retransmission times are compared to those occurs in the real wireless LAN or not but one can depend on this output to investigate the behavior of the simulation. These values of errors can be adjusted by changing (increasing or decreasing) the value of PERR value at beginning of the software statements, and may have very much possibility of errors or rarely errors in the simulation period.
The other printout is when hide all the above mentioned values. There are so many values for lamda and the corresponding values of the transmission channel utilization and the delay during the transmission process are printed. These values are statistical values, the number of samples is set to be 500 and for each value of lamda the corresponding average value of the throughput and the delay is printed. It was notice from the results that these values for the delay are closed to the theoretical and expected values, which give an increasing value for the delay with the increment in the load. But for the overall throughput we are expecting and increment of the throughput up to a peak value then a decreasing at the end with the increase in the load, not as we obtained an exponential decreasing graph. We observe that the graphs of the throughput has some changes by the changing the bit rate (increasing or decreasing), or changing the length of the packet frame length, and increasing the number of the samples taken for the statistical average values as shown in the attached sheets of the printout. Also changing the value of PERR which vary the possibility of number of errors occurring during the simulation study period did some of effects in the obtained results values.
The simulation software follow our model and this model depends on the characteristic and standard of the wireless LAN. The only assumptions those made are made for the message duration and the inter arrival times of the hosts which we assume them following the exponential distribution, and may be if they

follow another distribution, the simulation can results can better than what we got from this modeling and simulation.

By the way by analyzing in deep the software, one may realize from the results that for this values of throughput the transmission media is not perfectly utilized, and therefore there are many gaps of intervals in which the transmission media is idle. One may conclude that when the errors are presented this will affect the efficiency of the network, and also as the number of hosts increases the efficiency will drop further that the previous value because the possibility of the errors will increases.

Let us have another point of view for the results and look for a way to improve these results, especially by trying to fill the gaps of the interval time in the axis of the total time. By comparing the two protocols for the wired and the wireless. In the wired LANs there is the Back off time which stated from the CSMA/CD, when the media is busy the host wait for random time then start to transmit, and if again the media is busy the host can wait for another time and then start to transmit and so on…, . If we used this time in our simulation software we can result in better results than whose obtained by at least partially filling our gaps or some of these gaps of time. This will improve our utilization of the transmission media and may be better graph for the delay than what we got here by this simulation. But this not possible because the back off time was mentioned only in the CSMA/CD protocol for the wired LANs. This is one example one can also find another way of filling those gaps presented in our simulation software of five hosts, if we add something that is not mentioned in the CSMA/CA protocol specified for the wireless LAN.

CHAPTER FIVE

CONCLUSION

The study of the behavior of the wireless LAN may require so many advance methods. In this work use was made of a simple and reliable way by manipulating a

model which depends on the IEEE standard characteristics and its clear statements, from which the software was constructed and built.

In theory the shape of the graph for the delay in a wireless LAN is an increasing exponential function, as long as the load is increased. And for the throughput the curve is an increasing function up to a peak value and then tends to decrease with the increase in the load at the network. The results obtained show an increase in the delay with the increase in the load, and for the throughput a decrease as the load increase in the network. This is due to the presence of errors in the transmission media that greatly affect the obtained results. As shown in Chapter Four (Results and Discussion) there are intervals of time of the total time counter axis in which the transmission medium is idle and is not utilized by the hosts, and causes the throughput to be less than the expected value. These intervals of time can be decreased with the addition of some new statement in the MAC CSMA/CD protocol, such as the back-off time which is presented for the CSMA/CD protocol. This time increases the possibility of sending the packets when the channel is in idle state. Also it should be possible to find another way of utilizing the channel in the idle state or by sending two hosts at the same time if their destinations do not collide with each other for a significant long distance of transmission.

The above suggestions are suitable for small wireless LANs like the presently assumed network, which is suitable for small offices or a university campus, but not for a large Distribution System (DS) or when the network topology is complicated. This is because our simulation software was applied for a very small number of hosts. But when the number of hosts is large may be there are other suggestions that can help in achieving better utilization for the wireless LAN networks.

REFERENCES

1- William Stallings, “Wirelerss Communication and Networks”, Sixth edition, Prentice Hall, 2001

2- Andrew S. Tanenbaum, “Computer Networks”, Second edition, Prentice Hall PTR, 1988.

3- Ross N. William, “Painless Guide to CRC Error Detection Code”, Copy right (C), Ross William, 1993.

4- F. M, Aziz “Implementation and Analysis of Wireless LANs for High-Mobility Telematics”, M.Sc. Thesis, Virginia Polycentric and State University, Blacksburg, Virginia- USA, May 30, 2003

5- Srikant Sharma, “Analysis of 802.11`b MAC: A QoS, Fairness, and Performance Perspective”, Department of Computer Science, Stony Brook University, NY 11794-0044, USA, srikant@cs.sunysb.edu .

6- Slimane Ben Slimane and Mikael Gdlund, “Performance of Wireless LANs on Radio Channels”, Radio Communication System Group, Department of Signals, Sensors, and Systems, Royal Institute of Technology, S-100 44 Stockhom, Sweden, slimane@radio.kth.se, gidmi@ite.mh.se.